In The Claims:

1. (Currently amended) A computer program product for providing a secure, integrated device with dynamically selectable capabilities, the computer program product embodied on one or more computer-usable media and comprising:

computer-readable program code ~~means for operating~~ that is configured to operate a security core which provides security functions; ~~and~~

computer-readable program code ~~means for securely operably connecting~~ that is configured to establish a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each ~~securely~~ secure operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device;

computer-readable program code that is configured to securely perform a transaction using the secure integrated device;

computer-readable program code that is configured to detect whether all components participating in the securely performed transaction remain operably connected to the secure integrated device during the securely performed transaction; and

computer-readable program code that is configured to mark the securely performed transaction as not secure if one or more of the participating components fails to remain operably connected to the secure integrated device during the securely performed transaction.

2. (Original) The computer program product according to Claim 1, wherein selected ones of the operable connections are made using one or more buses of the secure integrated device.

3. (Original) The computer program product according to Claim 1, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

4. (Original) The computer program product according to Claim 3, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

5. (Original) The computer program product according to Claim 1, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

6. (Original) The computer program product according to Claim 1, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

7. (Currently amended) The computer program product according to Claim 1, wherein the computer-readable program code~~ means for securely operably connecting~~ that is configured to establish a secure, operable connection of one or more components to the security core further comprises computer-readable program code ~~means for authenticating~~ that is configured to authenticate the operably connected component to the security core.

8. (Currently amended) The computer program product according to Claim 7, wherein the computer-readable program code ~~means for authenticating~~ that is configured to authenticate provides a unique identifier of the operably connected component to the security core.

9. (Currently amended) The computer program product according to Claim 1, wherein the computer-readable program code ~~means for securely operably connecting~~ that is configured to establish a secure, operable connection of one or more components to the security core is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

10. (Currently amended) The computer program product according to Claim 7, wherein the computer-readable program code ~~means for authenticating~~ that is configured to authenticate is activated during execution of computer-readable program code stored on the

component, and wherein the execution of the stored computer-readable program code is activated by a hardware reset of the component.

11. (Currently amended) The computer program product according to Claim 7, wherein the computer-readable program code ~~means for authenticating~~ that is configured to authenticate is securely stored on the component.

12. (Currently amended) The computer program product according to Claim 7, further comprising computer-readable program code ~~means for authenticating~~ that is configured to authenticate the security core to the operably connected component.

13. (Currently amended) The computer program product according to Claim 7, wherein the computer-readable program code ~~means for authenticating~~ that is configured to authenticate the operably connected component further comprises computer-readable program code ~~means for using~~ that is configured to use public key cryptography.

14. (Currently amended) The computer program product according to Claim 12, wherein the computer-readable program code ~~means for authenticating~~ that is configured to authenticate the security core further comprises computer-readable program code ~~means for using~~ that is configured to use public key cryptography.

15. (Original) The computer program product according to Claim 1, wherein the secure integrated device is a pervasive computing device.

16. (Currently amended) The computer program product according to Claim 1, wherein one or more cryptographic keys are securely stored in each component, and wherein at least one of the securely stored keys is used by the computer-readable program code that is configured to establish a secure operable connection of each component to the security core ~~means for securely operably connecting each component~~.

17. (Original) The computer program product according to Claim 1, wherein one or more cryptographic keys are securely stored in the secure integrated device.

18. (Currently amended) The computer program product according to Claim 1, further comprising computer-readable program code ~~means for authenticating~~ that is configured to authenticate a user of the secure integrated device.

19. (Canceled).

20. (Currently amended) A computer program product for providing a secure, integrated device with dynamically selectable capabilities, the computer program product embodied on one or more computer-usable media and comprising:

computer-readable program code that is configured to operate a security core which provides security functions;

computer-readable program code that is configured to establish a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device;

computer-readable program code that is configured to securely perform a transaction using the secure integrated device;

~~The computer program product according to Claim 19, further comprising:~~

computer-readable program code ~~means for detecting~~ that is configured to detect whether all components participating in the securely performed transaction remain operably connected to the secure integrated device during the securely performed transaction; and

computer-readable program code ~~means for aborting~~ that is configured to abort the securely performed transaction if one or more of the participating components fails to remain operably connected to the secure integrated device during the securely performed transaction.

21. (Canceled).

22. (Currently amended) The computer program product according to Claim [[19]]1, wherein the computer-readable program code ~~means for securely performing~~ that is configured to securely perform a transaction further comprises computer-readable program code ~~means for~~

~~digitally notarizing~~ that is configured to digitally notarize, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device.

23. (Currently amended) A computer program product for providing a secure, integrated device with dynamically selectable capabilities, the computer program product embodied on one or more computer-usable media and comprising:

computer-readable program code that is configured to operate a security core which provides security functions;

computer-readable program code that is configured to establish a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

computer-readable program code that is configured to securely perform a transaction using the secure integrated device, wherein the computer-readable program code that is configured to securely perform a transaction further comprises computer-readable program code that is configured to digitally notarize, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, and ~~The computer program product according to Claim 22,~~ wherein the computer-readable program code ~~means for digitally notarizing~~ that is configured to digitally notarize further comprises:

computer-readable program code ~~means for authenticating~~ that is configured to authenticate the selected operably connected component to the security core;

computer-readable program code ~~means for computing~~ that is configured to compute, by the security core, a hash value over the output data stream;

computer-readable program code ~~means for hashing~~ that is configured to hash, by the security core, a combination of (1) the hash value and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block;

computer-readable program code ~~means for digitally signing~~ that is configured to digitally sign, by the security core, the hashed data block using a private key of the security core; and

computer-readable program code ~~means for providing~~ that is configured to provide the digitally signed hashed data block along with the combination as the digital notarization of the output data stream.

24. (Currently amended) The computer program product according to Claim 23, wherein the computer-readable program code ~~means for authenticating~~ that is configured to authenticate further comprises computer-readable program code ~~means for using~~ that is configured to use a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably connected component using a first private key associated with the selected operably connected component.

25. (Currently amended) A computer program product for providing a secure, integrated device with dynamically selectable capabilities, the computer program product embodied on one or more computer-usable media and comprising:

computer-readable program code that is configured to operate a security core which provides security functions;

computer-readable program code that is configured to establish a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

computer-readable program code that is configured to securely perform a transaction using the secure integrated device, wherein the computer-readable program code that is configured to securely perform a transaction further comprises computer-readable program code that is configured to digitally notarize, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, and ~~The computer program product according to Claim 22~~, wherein the computer-readable program code ~~means for digitally notarizing~~ that is configured to digitally notarize further comprises:

computer-readable program code ~~means for authenticating~~ that is configured to authenticate the selected operably connected component to the security core;

computer-readable program code ~~means for computing~~ that is configured to compute, by the security core, a hash value over each of a plurality of segments of the output data stream, wherein a boundary between segments is determined by an elapsed time value;

computer-readable program code ~~means for hashing~~ that is configured to hash, by the security core, a combination of (1) the hash value for each segment and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block for each segment;

computer-readable program code ~~means for digitally signing~~ that is configured to digitally sign, by the security core, the hashed data block for each segment using a private key of the security core; and

computer-readable program code ~~means for providing~~ that is configured to provide the digitally signed hashed data block for each segment along with the combination for each segment as the digital notarization of the segments which comprise the output data stream.

26. (Currently amended) The computer program product according to Claim 25, wherein the computer-readable program code ~~means for authenticating~~ that is configured to authenticate further comprises computer-readable program code ~~means for using~~ that is configured to use a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably connected component using a first private key associated with the selected operably connected component.

27. (Original) The computer program product according to Claim 25, wherein authenticity of selected ones of the digitally notarized segments of the output data stream may be separately verified using a public key of the security core.

28. (Currently amended) The computer program product according to Claim 23 or Claim 25, further comprising:

computer-readable program code ~~means for authenticating~~ that is configured to authenticate a user of the secure integrated device; and

computer-readable program code ~~means for including~~ that is configured to include an identification of the authenticated user in the combination.

29. (Original) The computer program product according to Claim 23 or Claim 25, wherein the private key of the security core is securely stored in the secure integrated device.

30. (Currently amended) The computer program product according to Claim 23, further comprising computer-readable program code ~~means for verifying~~ that is configured to verify authenticity of the output data stream by a receiver of the output data stream and the digitally signed hashed data block, using a public key of the security core, and ~~for concluding~~ to conclude that the output data stream is authentic if the verification succeeds.

31. (Currently amended) The computer program product according to Claim 30, wherein the computer-readable program code ~~means for verifying~~ that is configured to verify authenticity further comprises computer-readable program code that is configured to obtain ~~obtaining~~ the public key from a digital certificate of the security core.

32. (Currently amended) The computer program product according to Claim 30, wherein the computer-readable program code ~~means for verifying~~ that is configured to verify authenticity further comprises computer-readable program code that is configured to conclude ~~concluding~~ that the output data stream has not been tampered with if the verification succeeds.

33. (Currently amended) The computer program product according to Claim 1, further comprising computer-readable program code ~~means for dynamically revising~~ that is configured to dynamically revise functionality in a selected one of the securely operably connected components of the secure integrated device by securely applying a firmware update to the selected one, such that the security core can continue to vouch for the authenticity of the selected one.

34. (Currently amended) The computer program product according to Claim 1, wherein capabilities of the secure integrated device are dynamically revised by subsequent operation of the computer-readable program code ~~means for securely operably connecting~~ that is configured to establish a secure, operable connection of one or more components to the security core, the subsequent operation being activated upon operably connecting a new component to the security core, wherein the new component authenticates itself to the security core, with a result of the authentication being that the capabilities of the secure integrated device are thereby augmented with capabilities of the new component.

35. (Original) The computer program product according to Claim 1, wherein the security core is located on a selected one of the operably connected components, and wherein the security core and the selected one are connected to a common bus.

36. (Original) The computer program product according to Claim 1, wherein a second security core is located on a selected one of the operably connected components, and wherein the security core and the second security core operate in combination.

37-40. (Canceled).

41. (Currently amended) A system for providing a secure, integrated device with dynamically selectable capabilities, comprising:

a security core which provides security functions;

one or more components;

means for operating the security core; ~~and~~

means for establishing a secure, operable connection of ~~securely operably connecting~~ the components to the security core, such that the security core can vouch for authenticity of each ~~securely~~ secure operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device;

means for securely performing a transaction using the secure integrated device;

means for detecting whether all components remain operably connected to the secure integrated device during the securely performed transaction; and

means for marking the securely performed transaction as not secure if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction.

42. (Original) The system according to Claim 41, wherein selected ones of the operable connections are made using one or more buses of the secure integrated device.

43. (Original) The system according to Claim 41, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

44. (Original) The system according to Claim 43, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

45. (Original) The system according to Claim 41, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

46. (Original) The system according to Claim 41, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

47. (Currently amended) The system according to Claim 41, wherein the means for establishing a secure, operable connection of the components to the security core ~~securely operably connecting~~ further comprises means for authenticating the operably connected component to the security core.

48. (Original) The system according to Claim 47, wherein the means for authenticating provides a unique identifier of the operably connected component to the security core.

49. (Original) The system according to Claim 41, wherein the means for establishing a secure, operable connection of the components to the security core ~~securely operably connecting~~ is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

50. (Original) The system according to Claim 47, wherein the means for authenticating is activated during execution of instructions stored on the component, and wherein the execution of the stored instructions is activated by a hardware reset of the component.

51. (Original) The system according to Claim 47, wherein the means for authenticating are securely stored on the component.

52. (Original) The system according to Claim 47, further comprising means for authenticating the security core to the operably connected component.

53. (Original) The system according to Claim 47, wherein the means for authenticating the operably connected component further comprises means for using public key cryptography.

54. (Original) The system according to Claim 52, wherein the means for authenticating the security core further comprises means for using public key cryptography.

55. (Original) The system according to Claim 41, wherein the secure integrated device is a pervasive computing device.

56. (Currently amended) The system according to Claim 41, wherein one or more cryptographic keys are securely stored in each component, and wherein at least one of the securely stored keys is used by the means for establishing a secure, operable connection of the components to the security core ~~securely operably connecting each component~~.

57. (Original) The system according to Claim 41, wherein one or more cryptographic keys are securely stored in the secure integrated device.

58. (Original) The system according to Claim 41, further comprising means for authenticating a user of the secure integrated device.

59. (Canceled).

60. (Currently amended) A system for providing a secure, integrated device with dynamically selectable capabilities, comprising:

a security core which provides security functions;

one or more components;

means for operating the security core;

means for securely, operably connecting the components to the security core, such that the security core can vouch for authenticity of each secure, operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device;

means for securely performing a transaction using the secure integrated device;

~~The system according to Claim 59, further comprising:~~

means for detecting whether the components remain operably connected to the secure integrated device during the securely performed transaction; and

means for aborting the securely performed transaction if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction.

61. (Canceled).

62. (Currently amended) The system according to Claim [[59]]41, wherein the means for securely performing a transaction further comprises means for digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device.

63. (Currently amended) A system for providing a secure, integrated device with dynamically selectable capabilities, comprising:

a security core which provides security functions;

one or more components;

means for operating the security core;

means for establishing a secure, operable connection of the components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

means for securely performing a transaction using the secure integrated device, wherein the means for securely performing a transaction further comprises means for digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, and ~~The system according to Claim 62,~~ wherein the means for digitally notarizing further comprises:

means for authenticating the selected operably connected component to the security core;

means for computing, by the security core, a hash value over the output data stream;

means for hashing, by the security core, a combination of (1) the hash value and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block;

means for digitally signing, by the security core, the hashed data block using a private key of the security core; and

means for providing the digitally signed hashed data block along with the combination as the digital notarization of the output data stream.

64. (Original) The system according to Claim 63, wherein the means for authenticating further comprises means for using a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably

connected component using a first private key associated with the selected operably connected component.

65. (Currently amended) A system for providing a secure, integrated device with dynamically selectable capabilities, comprising:

a security core which provides security functions;

one or more components;

means for operating the security core;

means for establishing a secure, operable connection of the components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

means for securely performing a transaction using the secure integrated device, wherein the means for securely performing a transaction further comprises means for digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, and ~~The system according to Claim 62,~~ wherein the means for digitally notarizing further comprises:

means for authenticating the selected operably connected component to the security core;

means for computing, by the security core, a hash value over each of a plurality of segments of the output data stream, wherein a boundary between segments is determined by an elapsed time value;

means for hashing, by the security core, a combination of (1) the hash value for each segment and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block for each segment;

means for digitally signing, by the security core, the hashed data block for each segment using a private key of the security core; and

means for providing the digitally signed hashed data block for each segment along with the combination for each segment as the digital notarization of the segments which comprise the output data stream.

66. (Original) The system according to Claim 65, wherein the means for authenticating further comprises means for using a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably connected component using a first private key associated with the selected operably connected component.

67. (Original) The system according to Claim 65, wherein authenticity of selected ones of the digitally notarized segments of the output data stream may be separately verified using a public key of the security core.

68. (Original) The system according to Claim 63, further comprising:

means for authenticating a user of the secure integrated device; and means for including an identification of the authenticated user in the combination.

69. (Original) The system according to Claim 65, wherein the private key of the security core is securely stored in the secure integrated device.

70. (Original) The system according to Claim 65, further comprising means for verifying authenticity of the segments of the output data stream by a receiver of the segments of the output data stream and the digitally signed hashed data blocks for the segments, using a public key of the security core, and for concluding that each segment of the output data stream is authentic if the verification succeeds.

71. (Original) The system according to Claim 70, wherein the means for verifying authenticity further comprises obtaining the public key from a digital certificate of the security core.

72. (Original) The system according to Claim 70, wherein the means for verifying authenticity further comprises concluding that the output data stream has not been tampered with if the verification succeeds.

73. (Currently amended) The system according to Claim 41, further comprising:

means for dynamically revising functionality in a selected one of the ~~securely~~ secure, operably connected components of the secure integrated device by securely applying a firmware update to the selected one; and

means for requiring the selected one to re-authenticate itself to the security core, such that the security core can continue to vouch for the authenticity of the selected one.

74. (Currently amended) The system according to Claim 41, wherein capabilities of the secure integrated device are dynamically revised by subsequent operation of the means for establishing a secure, operable connection of the components to the security core ~~securely operably connecting~~, the subsequent operation being activated upon operably connecting a new component to the security core, wherein the new component authenticates itself to the security core, with a result of the authentication being that the capabilities of the secure integrated device are thereby augmented with capabilities of the new component.

75. (Original) The system according to Claim 41, wherein the security core is located on a selected one of the operably connected components, and wherein the security core and the selected one are connected to a common bus.

76. (Original) The system according to Claim 41, wherein a second security core is located on a selected one of the operably connected components, and wherein the security core

and the second security core each provide security functions for one or more components of the secure integrated device.

77-80. (Canceled).

81. (Currently amended) A method of providing a secure, integrated device with dynamically selectable capabilities, comprising ~~step of~~:

operating a security core which provides security functions; ~~and~~

establishing a secure, operable connection of ~~securely operably connecting~~ one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device;

securely performing a transaction using the secure integrated device;

detecting whether all components remain operably connected to the secure integrated device during the securely performed transaction; and

marking the securely performed transaction as not secure if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction.

82. (Original) The method according to Claim 81, wherein selected ones of the operable connections are made using one or more buses of the secure integrated device.

83. (Original) The method according to Claim 81, wherein selected ones of the operable connections are made using a wireless connection between respective ones of the components and the security core.

84. (Original) The method according to Claim 83, wherein the wireless connections use Secure Sockets Layer (SSL) data encryption or an equivalent which provides mutual authentication of both endpoints, negotiation of a time-limited key agreement with secure passage of a selected encryption key, and periodic renegotiation of the time-limited key agreement with a new encryption key.

85. (Original) The method according to Claim 81, wherein selected ones of the secure operable connections are provided when the security core is manufactured.

86. (Original) The method according to Claim 81, wherein the components comprise one or more of (1) input/output components and (2) application processing components.

87. (Currently amended) The method according to Claim 81, wherein ~~the step of securely operably connecting~~ establishing a secure, operable connection of one or more components to the security core further comprises ~~the step of~~ authenticating the operably connected component to the security core.

88. (Currently amended) The method according to Claim 87, wherein ~~the step of~~ authenticating the operably connected component to the security core provides a unique identifier of the operably connected component to the security core.

89. (Currently amended) The method according to Claim 81, wherein ~~the step of securely operably connecting~~ establishing a secure, operable connection of one or more components to the security core is activated by a hardware reset of the component, and wherein the hardware reset is activated by operably connecting of the component.

90. (Currently amended) The method according to Claim 87, wherein ~~the step of~~ authenticating the operably connected component to the security core is activated during execution of instructions stored on the component, and wherein the execution of the stored instructions is activated by a hardware reset of the component.

91. (Currently amended) The method according to Claim 87, wherein instructions for performing the authenticating of the operably connected component to the security core ~~step~~ are securely stored on the component.

92. (Currently amended) The method according to Claim 87, further comprising ~~the step of~~ authenticating the security core to the operably connected component.

93. (Currently amended) The method according to Claim 87, wherein ~~the step of~~ authenticating the operably connected component to the security core further comprises using public key cryptography.

94. (Currently amended) The method according to Claim 92, wherein ~~the step of~~ authenticating the security core to the operably connected component further comprises using public key cryptography.

95. (Original) The method according to Claim 81, wherein the secure integrated device is a pervasive computing device.

96. (Original) The method according to Claim 81, wherein one or more cryptographic keys are securely stored in each component, and wherein at least one of the securely stored keys is used by the step of securely operably connecting each component.

97. (Original) The method according to Claim 81, wherein one or more cryptographic keys are securely stored in the secure integrated device.

98. (Currently amended) The method according to Claim 81, further comprising ~~the step of~~ authenticating a user of the secure integrated device.

99. (Canceled) .

100. (Currently amended) A method of providing a secure, integrated device with dynamically selectable capabilities, comprising:

operating a security core which provides security functions;

establishing a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each securely operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device;

securely performing a transaction using the secure integrated device;

~~The method according to Claim 99, further comprising the steps of:~~

detecting whether the components remain operably connected to the secure integrated device during the securely performed transaction; and

aborting the securely performed transaction if one or more of the components fails to remain operably connected to the secure integrated device during the securely performed transaction.

101. (Canceled).

102. (Currently amended) The method according to Claim [[99]]81, wherein ~~the step of~~ securely performing a transaction further comprises ~~the step of~~ digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device.

103. (Currently amended) A method of providing a secure, integrated device with dynamically selectable capabilities, comprising:

operating a security core which provides security functions;

establishing a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each secure operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

securely performing a transaction using the secure integrated device, wherein securely performing a transaction further comprises digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, ~~The method according to Claim 102,~~ wherein ~~the step of~~ digitally notarizing further comprises~~ the steps of~~:

authenticating the selected operably connected component to the security core;

computing, by the security core, a hash value over the output data stream;

hashing, by the security core, a combination of (1) the hash value and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block;

digitally signing, by the security core, the hashed data block using a private key of the security core; and

providing the digitally signed hashed data block along with the combination as the digital notarization of the output data stream.

104. (Currently amended) The method according to Claim 103, wherein ~~the step of~~ authenticating further comprises using a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably connected component using a first private key associated with the selected operably connected component.

105. (Currently amended) A method of providing a secure, integrated device with dynamically selectable capabilities, comprising:

operating a security core which provides security functions;

establishing a secure, operable connection of one or more components to the security core, such that the security core can vouch for authenticity of each secure operably connected component, wherein the security core and the operably connected components thereby comprise the secure integrated device; and

securely performing a transaction using the secure integrated device, wherein securely performing a transaction further comprises digitally notarizing, by the security core, an output data stream created by a selected one of the operably connected components of the secure integrated device, ~~The method according to Claim 102,~~ wherein the digitally notarizing ~~step~~ further comprises ~~the steps of~~:

authenticating the selected operably connected component to the security core;

computing, by the security core, a hash value over each of a plurality of segments of the output data stream, wherein a boundary between segments is determined by an elapsed time value;

hashing, by the security core, a combination of (1) the hash value for each segment and (2) the unique identifier of the selected operably connected component, thereby creating a hashed data block for each segment;

digitally signing, by the security core, the hashed data block for each segment using a private key of the security core; and

providing the digitally signed hashed data block for each segment along with the combination for each segment as the digital notarization of the segments which comprise the output data stream.

106. (Currently amended) The method according to Claim 105, wherein the authenticating ~~step~~ further comprises using a unique identifier of the selected operably connected component, where the unique identifier is digitally signed by the selected operably connected component using a first private key associated with the selected operably connected component.

107. (Original) The method according to Claim 105, wherein authenticity of selected ones of the digitally notarized segments of the output data stream may be separately verified using a public key of the security core.

108. (Currently amended) The method according to Claim 105, further comprising ~~the steps of~~:

authenticating a user of the secure integrated device; and

including an identification of the authenticated user in the combination.

109. (Original) The method according to Claim 103, wherein the private key of the security core is securely stored in the secure integrated device.

110. (Currently amended) The method according to Claim 105, further comprising ~~the step of~~ verifying authenticity of the segments of the output data stream by a receiver of the segments of the output data stream and the digitally signed hashed data blocks for the segments, using a public key of the security core, and concluding that each segment of the output data stream is authentic if the verification succeeds.

111. (Currently amended) The method according to Claim 110, wherein ~~the step of~~ verifying authenticity further comprises obtaining the public key from a digital certificate of the security core.

112. (Currently amended) The method according to Claim 110, wherein ~~the step of~~ verifying authenticity further comprises concluding that the output data stream has not been tampered with if the verification succeeds.

113. (Currently amended) The method according to Claim 81, further comprising ~~the steps of~~:

dynamically revising functionality in a selected one of the ~~securely~~ secure operably connected components of the secure integrated device by securely applying a firmware update to the selected one; and

requiring the selected one to re-authenticate itself to the security core, such that the security core can continue to vouch for the authenticity of the selected one.

114. (Currently amended) The method according to Claim 81, wherein capabilities of the secure integrated device are dynamically revised by subsequent operation of ~~the securely operably connecting step~~ establishing a secure, operable connection of one or more components to the security core, the subsequent operation being activated upon operably connecting a new component to the security core, wherein the new component authenticates itself to the security core, with a result of the authentication being that the capabilities of the secure integrated device are thereby augmented with capabilities of the new component.

115. (Original) The method according to Claim 81, wherein the security core is located on a selected one of the operably connected components, and wherein the security core and the selected one are connected to a common bus.

116. (Original) The method according to Claim 81, wherein a second security core is located on a selected one of the operably connected components, and wherein the security core and the second security core each provide security functions for one or more components of the secure integrated device.

117-120. (Canceled).